Safety Science 84 (2016) 181–189

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

Should healthcare providers do safety cases? Lessons from a cross-industry review of safety case practices

Mark A. Sujan [a,*], Ibrahim Habli [b], Tim P. Kelly [b], Simone Pozzi [c], Christopher W. Johnson [d]

[a] Warwick Medical School, University of Warwick, Coventry CV4 7AL, UK
[b] Department of Computer Science, University of York, York YO10 5GH, UK
[c] Deep Blue Research & Consulting, Rome, Italy
[d] School of Computing Science, University of Glasgow, Glasgow, Scotland, UK

ARTICLE INFO

Article history:
Received 26 July 2015
Received in revised form 17 November 2015
Accepted 14 December 2015
Available online 2 January 2016

Keywords:
Safety case
Regulation
Certification
Safety management
Healthcare

ABSTRACT

Healthcare organisations are often encouraged to learn from other industries in order to develop proactive and rigorous safety management practices. In the UK safety–critical industries safety cases have been used to provide justification that systems are acceptably safe. There has been growing interest in healthcare in the application of safety cases for medical devices and health information technology. However, the introduction of safety cases into general safety management and regulatory practices in healthcare is largely unexplored and unsupported. Should healthcare as an industry be encouraged to adopt safety cases more widely? This paper reviews safety case practices in six UK industries and identifies drivers and developments in the adoption of safety cases. The paper argues that safety cases might best be used in healthcare to provide an exposition of risk rather than as a regulatory tool to demonstrate acceptable levels of safety. Safety cases might support healthcare organisations in establishing proactive safety management practices. However, there has been criticism that safety cases practices have, at times, contributed to poor safety management and standards by prompting a "tick-box" and compliance-driven approach. These criticisms represent challenges for the adoption of safety cases in healthcare, where the level of maturity of safety management systems is arguably still lower than in traditional safety–critical industries. Healthcare stakeholders require access to education and guidance that takes into account the specifics of healthcare as an industry. Further research is required to provide evidence about the effectiveness of safety cases and the costs involved with the approach.

1. Introduction

Patient safety is an area of significant public concern. In the UK, there has been much media coverage of the findings of the Public Inquiry into the failings at Mid Staffordshire NHS Foundation Trust. The report suggests that between 2005 and 2009 as many as 1200 patients died needlessly as a result of inadequate and often appalling standards of care (Francis, 2013). There is evidence from a wide range of countries and health systems that suggests that patients around the world are suffering preventable adverse events (Vincent et al., 2001; Davis et al., 2002; Baker et al., 2004; de Vries et al., 2008; Thomas et al., 2000; Brennan et al., 1991). Adverse events cause unnecessary suffering, and they also have significant financial implications resulting from additional bed days and extended care requirements of patients, as well as from increased insurance and litigation costs (Vincent et al., 2001; Ovretveit, 2009).

Healthcare organisations have been encouraged to consider lessons from safety management in safety–critical industries in order to improve the safety of patients and reduce the number of adverse events (Department of Health, 2000; Kohn et al., 2000). For example, in the English National Health Service (NHS) lessons learned about incident reporting in aviation have contributed to the establishment of a national incident reporting system (National Reporting and Learning System) (Carruthers and Phillip, 2006). There is also an increasing number of documented examples of the application of risk analysis methods such as Failure Mode and Effects Analysis (FMEA), which healthcare organisations are becoming more familiar with (Apkon et al., 2004; Burgmeier, 2002; Steinberger et al., 2009; Sujan and Felici, 2012).

In UK safety–critical industries, manufacturers and operators of safety–critical systems, such as nuclear power plants and

* Corresponding author. Tel.: +44 24765 72941.
E-mail addresses: m-a.sujan@warwick.ac.uk (M.A. Sujan), Ibrahim.Habli@york.ac.uk (I. Habli), Tim.Kelly@york.ac.uk (T.P. Kelly), Simone.Pozzi@dblue.it (S. Pozzi), Christopher.Johnson@glasgow.ac.uk (C.W. Johnson).

http://dx.doi.org/10.1016/j.ssci.2015.12.021
0925-7535/

petrochemical facilities, have to submit a safety case to the respective regulatory authority (Maguire, 2006). In these industries safety cases provide an accepted means for demonstrating and assessing that a disciplined and effective approach to managing risk has been adopted, and that the resulting system can be regarded with confidence as acceptably safe (Bloomfield et al., 2012a). However, there has also been criticism of the safety case approach suggesting that poor safety case practices were a key contributor to accidents by prompting a "tick-box" and overly compliance-driven approach to safety (Haddon-Cave, 2009). Studies also suggest that there was a lack of evidence about their effectiveness as a tool for regulatory oversight (Leveson, 2011; Steinzor, 2011).

In healthcare there has been recent interest in the safety case concept, in particular for medical devices (Sujan et al., 2007) such as infusion pumps (FDA, 2014), and for health information technology (Health and Care Information Centre, 2013a, 2013b; Sujan et al., 2013). However, there is little established evidence about the role of safety cases for improving safety management practices in healthcare more widely (Sujan et al., 2015). There is also relatively little guidance on safety case use that is based on lessons across different industries rather than being very industry-specific. This lack of evidence and guidance is particularly problematic since safety management practices and the regulatory context in healthcare differ significantly from other safety–critical industries. Safety management in healthcare is arguably still largely driven by a reactive mindset and a regulatory approach that relies on routinely collected outcome data (such as mortality rates). There is a threat that within such a culture and environment safety cases might be perceived as another document-producing regulatory tool, or as a replacement to actual proactive thinking about patient safety risks.

Are safety cases a potential threat to mindful safety management or simply a necessary evil, or do safety cases have the potential to make a positive contribution to the development of more systematic and rigorous safety management practices in healthcare under the right circumstances? This paper presents lessons from a study (Bloomfield et al., 2012a) that reviewed the application of safety cases in six safety–critical industries (automotive, civil aviation, defence, nuclear, petrochemical and railways). The paper analyses drivers and developments in the adoption of safety cases across these industries. Based on such a broad, cross-industry review of safety case practices, the paper then examines critically challenges, lessons and prerequisites for the potential widespread and systematic development of safety cases within healthcare.

The paper is structured as follows. Section 2 briefly summarises the conceptual background to safety cases. Section 3 reflects on a review of safety case practices in six different industries, and identifies lessons across these industries for the adoption of safety cases. Section 4 briefly reviews the emerging use of safety cases in healthcare. Section 5 discusses the findings of the cross-industry analysis and identifies opportunities and challenges for the adoption of safety cases in healthcare. Section 6 concludes with the main implications for practice and for research.

2. Safety cases

Many of the current regulatory approaches in the UK require that manufacturers and operators of safety–critical systems demonstrate that they have adopted a thorough and systematic process for understanding proactively the risks associated with their systems and to control these risks appropriately. With these approaches the regulator formulates goals, but the demonstration that the goals have been achieved is left to the manufacturers and operators of systems. This provides them with the flexibility to argue their case taking into account the specific context and any technological advances. In the UK, these duties are often fulfilled through the use of safety cases. This current regulatory approach is the result of a shift from compliance-based to more goal-based regulatory approaches over the past 20 years. Under a predominantly prescriptive regulatory regime, manufacturers and operators claim safety through the satisfaction of specific standards and technical requirements specified by the regulator, rather than by demonstrating that certain higher-level goals have been met. The compliance-based approach has been criticised for prompting bureaucratic practices of safety management, where risks may not be properly understood, and for potentially hindering progress in industries that are driven by technological innovations (Hawkins et al., 2013; Habli and Kelly, 2006; Bishop et al., 2004). The goal-based approach aims to overcome these shortcomings of prescriptive regulatory regimes by providing both more responsibility as well as more flexibility to operators of systems.

The purpose of a safety case can be described as providing a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is acceptably safe for a given application in a given context (UK Ministry of Defence, 2007). A key characteristic of the safety case is a risk-based argument and corresponding evidence. This is intended to demonstrate that all risks associated with a particular system have been identified, that appropriate risk controls have been put in place, and that there are appropriate processes in place to monitor the effectiveness of the risk controls and the safety performance of the system on an on-going basis. The argument and evidence in safety cases are then examined and challenged, typically by independent safety assessors, as part of the overall safety assessment or certification process. Safety cases are usually confidential, but there are publicly available safety cases (see for example the Safety Case Repository (Dependability Research Group University of Virginia). The literature also includes descriptions of real safety case developments, as well as suggestions for high-level arguments and argument strategies (for example Barker et al., 1997; Chen et al., 2014; Chinneck et al., 2004; Habli et al., 2010). The use of safety cases is an accepted best practice in UK safety–critical industries, and is adopted by companies as a means of providing rigour and structure to their safety management systems. This is in line with recommendations provided by Lord Cullen in the highly influential Public Inquiry into the Piper Alpha oil platform explosion (The Honourable Lord Cullen, 1990). The report emphasises that meeting regulatory requirements should only be a secondary function of the safety case. The safety case should, first and foremost, provide assurance to the operators of safety–critical systems themselves that they have followed a systematic and thorough approach to ensure that their systems are safe (The Honourable Lord Cullen, 1990).

However, safety cases are not a panacea for successful safety management, and there has been criticism of the approach. It is important to critically review the lessons, criticisms and challenges of safety case practice in order to make suggestions for the meaningful adoption of safety cases in other industries, such as healthcare.

3. Review of safety case practices in six safety–critical industries

3.1. Aims, methodology and limitations

The recent interest in safety cases from industries like healthcare, which have little practical experience with the concept, justifies a longitudinal study into existing "good practices" as well as potential concerns. A review of safety case practices across different industries was undertaken (Bloomfield et al., 2012a, 2012b). The aim of the review was to document the different regulatory contexts, the key developments and drivers, and the types of safety cases and their content for each industry in order to provide an

evidence-based input to the current debate around safety cases and their potential application in novel domains such as healthcare.

The review considered six safety–critical industries: automotive, civil aviation, defence, nuclear, petrochemical and railways. These were chosen to constitute a set of representative traditional safety–critical industries as well as an industry that has recently begun to show an interest in the adoption of safety cases (automotive). A review template to be used for all industries was developed and agreed during project meetings. The review template suggested description of the following broad topics for each industry: regulatory context and best practice, developments and drivers, types of safety cases and content, and key lessons. Rapid, narrative literature reviews were conducted for each industry by experts in the respective industry during January–March 2011. As opposed to systematic reviews, there is not necessarily an agreed definition of what constitutes a rapid review. The purpose of the reviews in this project was to provide within a reasonable period of time an evidence summary of safety case use across the different industries. The scope of the reviews was limited to domains, standards and guidelines in which safety cases have played an important role in the safety certification or assessment processes. Such an approach bears the risk of missing some information, and of introducing bias during the critical appraisal. In order to reduce these risks, each industry review was internally cross-reviewed by two other experts. A stakeholder workshop was conducted in March 2011 to validate and consolidate the findings. The workshop brought together participants from industry and from healthcare. The programme and the presentations of the workshop are available for download (Workshop on Safety Cases – Lessons from Industry and Application in Healthcare, 2011).

3.2. Cross-industry analysis

The detailed industry reviews are publicly available for download (Bloomfield et al., 2012b), and are not repeated here. Table 1 summarises for each industry the key lessons and challenges for safety case use that were identified from the individual industry reviews. In this sub-section these findings from each individual industry are analysed in order to identify common themes across the industries: the role of the regulator, drivers behind the adoption of safety cases, the demonstration of acceptable levels of risk, the practicality of review of safety cases, and the problem of providing empirical evidence of the effectiveness of safety cases.

3.2.1. Role of the regulator

Independent national regulatory bodies typically provide technical requirements, guidance and advice to manufacturers and operators of systems, but they also possess the powers to issue warnings and withhold or withdraw permission to operate a system.

The role of the regulator and the approach taken was a key influence in the adoption of safety cases. The inclusion of safety cases in the regulatory framework set a mandate for the industry. For example, the HSE requires the development of safety cases (or safety reports) from high-risk offshore and on-shore petrochemical installations as outlined in the Offshore Installations (Safety Case) Regulations 2005 (The Offshore Installations (Safety Case) Regulations, 2005) and the Control of Major Accident Hazards Regulation 1999 (COMAH) HSE, 1999. In the UK defence sector, the development and acceptance of safety cases as a means of assuring and certifying the acceptable safety of UK defence-related equipment has become widespread since the mid-1990s. There was a notable change in 1996 from Issue 1 to Issue 2 of Defence Standard 00-56 (Safety Management Requirements for Defence Related Systems, current Issue 4 2007) (UK Ministry of Defence, 2007) to include the concept of safety cases as an essential part of the procurement of UK defence related system. In the time since Issue 2 of Def Stan 00-56, the Ministry of Defence's own internal safety management standards (documented through Joint Service Publications – JSPs) have all gradually been updated to include the requirements for the development and acceptance of safety cases. Examples include JSP 430 (UK Ministry of Defence, 1996) requiring safety cases for ships and ship systems, JSP 553 (UK Ministry of Defence, 2003) requiring safety cases for military aircraft, and JSP 454 (UK Ministry of Defence, 2002) requiring safety cases for land systems. The existence of clear regulatory standards and clear definitions facilitates a practice of producing explicit and structured safety arguments.

However, the shift from prescriptive towards a goal-based regulatory paradigm has caused confusion, at times, within the industries, and detailed guidance and input by the regulator was required. The HSE, for example, acknowledged that there were new challenges under the COMAH legislation, in particular around the concept of "reasonably practicable" to determine whether risks had been adequately controlled (HSE) (see discussion on acceptable levels of risk below). The lack of experience and expertise with the safety case approach presents a further threat to its successful adoption. This relates not only to manufacturers and operators of systems, but also to the regulator. Regulatory bodies as well as industry stakeholders require education and training in order to implement and assess safety cases meaningfully. The lack of experience can also lead to the development of safety cases that are overly complex, that lack focus, and that are developed predominantly for the purpose of regulatory compliance.

In those instances where these challenges are overcome, safety cases have the potential to support the industries in managing safety in complex and dynamic environments across organisational boundaries. Industry best practice integrates the safety case as a key element in the communication between regulators and system operators, and in the safety management systems of the organisations. Safety cases are developed for both equipment and service levels to ensure an integrated system-wide view. They are required to be continuously updated and maintained as living and accurate documentation of the risks and the approach to dealing with them.

3.2.2. Drivers: accidents and increasing economic, organisational and technological change

The history of safety cases and safety case legislation in high-risk industries in the UK has been closely linked to the occurrence of high profile accidents. However, each industry was also subject to significant economic, organisational and technological changes within the industry that were then reflected in the approach taken to ensure continuing safety of the systems operated. The safety case approach was adopted in the different industries to provide a flexible yet clear regulatory framework able to ensure continuing safety in complex, fragmented and technologically driven systems.

In the petrochemical industry, the 1976 Seveso accident at a small chemical manufacturing facility in Italy resulted in the development of legislation aimed at the prevention and control of major accidents. The Public Inquiry into the Piper Alpha oil platform explosion (1988) The Honourable Lord Cullen, 1990 resulted in the adoption of a formal safety case requirement in the UK offshore industry. These accidents have been covered widely in the media, and their impact was industry-wide. This, in turn, prompted a wider discussion about the risks society is willing to tolerate in exchange for the benefits that such endeavours bring. In the UK, for example, the HSE published its criteria for decisions related to the regulation of risk in the context of changes in the preferences, values and expectations of society (HSE; Health and Safety Executive, 2001).

Table 1
Summary of key lessons and challenges for safety case practice identified from individual industry and healthcare reviews.

Industry	Key lessons and challenges for safety case practice identified
Automotive	*Increased focus through standardisation*: although the concept of a safety case was considered in earlier automotive safety guidelines (MISRA, 2007), the international standard ISO 26262 has significantly increased interest within the automotive safety industry in how safety arguments and evidence should be generated, documented, reviewed and maintained for automotive systems *Process focus and lack of industry experience with safety cases*: experience to date suggests that the primary focus of many of the documented safety cases for ISO 26262-compliant systems and components remains on processes (Birch et al., 2013). In extreme cases, this can result in bulky documentation that does little more than comply with the letter of the standard. Other characteristics have reduced the effectiveness of certain ISO 26262-compliant safety cases including: lack of focus and brevity; unnecessary repetition of information available elsewhere; and the use of inappropriate means of expression *Lack of published evidence*: currently, there is neither published evidence nor consensus within the industry on the real value of an automotive safety case, particularly when a safety process is compliant with ISO 26262. On the one hand, some stakeholders in the industry are treating the safety case as a repository of the work products generated from the safety lifecycle phases. One the other hand, other stakeholders are emphasising the role of the argument in showing how and why the work products (i.e. evidence) support the overarching claim that residual risks are acceptable and the importance of the timely generation of well-focussed safety arguments that are capable of improving both the development and assessment of automotive E/E systems
Civil aviation	*Fragmentation across the industry*: there is a need for integration between compliance-based and performance-based certification in order to reduce the gap between the assessment of airborne and ground-based systems. *Trade off between clarity and brevity*: given the complex technical contents of typical aviation safety cases, it is difficult to achieve the right balance between clarity and brevity. Most safety cases require a good understanding of system design and operational aspects. This understanding is hard to fully provide through the safety case report on its own *Resources required for adequate regulatory oversight*: regulatory bodies may find it difficult to provide sufficient numbers of human resources and with the appropriate domain knowledge to complete the review of safety cases. This may threaten their ability to execute their regulatory oversight function *Integration of safety cases into safety management activities*: EUROCONTROL states that the safety case should "*provide an adequate means of obtaining regulatory approval for the service or project concerned*" (Eurocontrol, 2006). However, a safety case does not constitute the only communication and coordination means between the service provider and the regulator. Other coordination processes are needed to ensure a continuous discussion of safety relevant issues. These processes are often poorly integrated with the safety case. This may result in the safety case being developed for mere compliance
Defence	*Substantial body of experience*: there is a substantial body of experience with safety case development within the UK defence domain. The domain has now lived with the cross-service requirement for safety cases for over fifteen years. As the Nimrod Review Report discusses, in this period there have been examples of poor safety cases alongside positive examples (Haddon-Cave, 2009). There is therefore much to learn from safety case practice in the UK defence domain *Clarity of approach*: positive features to observe include clear regulatory standards (such as Defence Standard 00-56), clear definitions, and the practice of producing explicit and structured safety arguments *Risk of complacency*: negative experiences to note include where safety case development appears to have become a 'paper exercise' through lack of stakeholder engagement, where the focus of safety management has been on maintaining safety case argumentation rather than maintaining the safety of the system, and where safety cases have not been used or allowed to influence and change practice *Lack of organisational support*: Further barriers to effective safety case use are practices where there has been insufficient organisational support for the MoD's many roles with respect to safety cases (customer, operator, regulator, owner) *Hierarchy of safety cases*: the Defence domain has evolved a clear understanding of the difference between equipment safety cases, and wider operational safety cases, and that a hierarchy of safety cases are sometimes required in order to establish an overall safety case
Nuclear	*Substantial body of experience*: the nuclear industry was the first industry in the UK to adopt the safety case approach with the Nuclear Installations Act 1965. Safety cases reflect accepted best practice, and a shared view of how safety of nuclear installations should be justified *Clarity of approach*: the Office for Nuclear Regulation has produced detailed Safety Assessment Principles (SAP) that set out what kind of information should be contained in nuclear safety cases. These SAPs are complemented by Technical Assessment Guides (TAG), which provide guidance on the interpretation and application of the SAPs (Office for Nuclear Regulation, 2014a, 2014b) *Slower rate of change*: drivers for the adoption of safety cases and structured safety management approaches in the nuclear industry include technological developments, changes to the energy market, and a number of accidents and incidents. However, the overall rate of change in the industry is slow compared to other industries *Qualities of and problems with safety cases*: safety cases should be intelligible, valid, complete, evidential, robust, integrated, balanced and forward looking. The ONR has identified common short-comings with respect to all of these qualities, and has updated the guidance on 'The purpose, scope and content of safety cases' (NS-TAST-GD-051 Revision 3) (Office for Nuclear Regulation, 2013)
Petrochemical	*Lack of published evidence*: there is little published evidence that safety cases have made an improvement to safety performance in the petrochemical industry (HSE, 2006a). However, their application, in much the same way as for accident investigation, has high face validity. Certainly, it would be difficult to argue that reviewing hazards and assessing risks could have anything other than a positive impact on safety performance *Resource implications*: safety report development is a potentially onerous activity for the establishments concerned. This is particularly the case in a goal-setting environment where the onus is on the operators to demonstrate that they are managing risk. There may be a danger, for example, of an organisation employing an external consultancy to develop a standard report that does little to engage the operator in the review of safety risks at their facility *Low probability, high consequence events*: A continuing challenge is dealing with the low probability nature of the major accidents that the safety report seeks to address. The industry is currently engaged in an effort to identify safety indicators that may more accurately indicate sites that are vulnerable to major accidents (HSE, 2006b) *Safety case maintenance*: ideally, safety reports would be living documents; continuously maintained as a risk register and a demonstration that the site is managing safety. However, the requirement for demonstration in relation to the ALARP concept means that reports often run to several hundred pages. They are typically complex documents that take up considerable site time and effort to develop. It may be challenging to sustain such a level of effort without regulatory pressure. Questions may also be asked whether in certain situations the focus on safety report development may detract from the day-to-day running of the plant
Railway	*Safety management in a fragmented, mixed economy*: the introduction of the safety case regime onto the UK's railways was driven by and concurrent with privatisation. There has been much debate about whether the fragmentation and consequent communication difficulties due to privatisation were contributory causes of the Southall and Ladbroke Grove disasters, and whether rail safety has improved or not since privatisation. One study suggested that a steady improvement in rail safety, as evidenced by a continuing decline in significant train accidents per unit distance travelled, had continued through the period of privatisation (Evans, 2007). It is likely that the safety case regime and its emphasis on safety management and risk control had in fact contributed to maintaining this trend, despite the negative impact of the fragmentation of British Rail assumed or argued for by many critics, particularly in technical journalism

Table 1 (*continued*)

Industry	Key lessons and challenges for safety case practice identified
	Lack of published evidence: there is little published evidence to support the proposition that safety cases have made a significant improvement to safety performance on Britain's railways. It may be very difficult to isolate the safety case regime from other potentially relevant factors in the face of the second order change facing the railway industry after 1994. However, there are views inside the industry suggesting that the application of the constituent parts of a safety case regime appeared to add value. It is possible that the UK's railway safety case regime assisted in maintaining safety through the serious upheavals associated with privatisation or part privatisation *Communication and collaboration among stakeholders*: one of the strengths of the UK Rail safety case regime was the system of assuring that the Infrastructure Controller reviewed and approved the safety cases of its operators. Critics of the system might say that this was merely ensuring an element of cohesion that would not have had to be enforced if the industry had not been fragmented by privatising it in the way that this was done. However, the complexity of modern industrial systems is such that collaboration between different organisations cannot be avoided in the delivery of any substantial service and systems for communication and sharing of data become essential. The safety case regime may have contributed to ensuring that resource was committed to the necessary level of co-operation at all levels
Healthcare	*Learning from practices within safety–critical industries*: the use of safety cases in healthcare is a recent phenomenon (Ray and Cleaveland, 2013; Despotou et al., 2012). Far from being an accepted best practice, the safety case approach is being trialled for small subsets of the healthcare system, which tend to be close to the traditional engineering tradition. In these areas, learning from best practices in other industries and review of their respective standards and approaches to safety management, have driven the current developments *Low maturity of safety management practices*: it could be argued that safety management practices in healthcare at present are less mature than those in other safety–critical industries. The introduction of goal-based approaches to regulation including the development of safety cases may have the potential to contribute to a more structured and rigorous approach to safety management in this industry *Education and training*: a significant threat to the successful uptake of the safety case approach is the lack of experience with the concept and the lack of expertise both within the regulatory bodies as well as among the stakeholders within the domain. Education and training for regulators, manufacturers, and service providers, as well as research evidence about the efficacy of the approach will be essential prerequisites for spreading the approach to the wider healthcare sector

Similarly, in the railway sector high profile accidents played an important role in shaping the management and oversight of safety. For example, the 1987 fire on an escalator at King's Cross on the London Underground and the 1988 Clapham main line derailment led to Public Enquiry reports (Fennell, 1998; Hidden, 1989) that implemented fundamental changes in the assessment of risk and management of safety on urban and main line railways. A further important driver for the adoption of safety cases in the UK railway industry was the introduction of privatisation to the surface railways in the UK and part-privatisation on the London Underground, which led to a period of commercial instability and insolvency in both cases. The Railways (Safety Case) Regulations 1994 (The Railways (Safety Case) Regulations, 1994) were adopted in order to meet the safety management challenges in a fragmented and mixed economy.

In the nuclear industry, the Windscale fire in 1957 led to the Nuclear Installations Act 1959 (with revision in 1965) that introduced a licensing scheme along with the requirement for the production of a safety case. A further driver for the adoption of safety cases were technical problems and high costs associated with the construction of advanced gas-cooled reactors, which prompted the UK Central Electricity Generating Board (CEGB) to consider the adoption of the American Pressurised Water Reactor (APW) design. Subsequently, a Public Inquiry was set up in 1983 to review the acceptability of the APW design (Layfield, 1987). This inquiry was based largely on the Pre-Construction Safety Case, and took almost two years to complete. The licensing process for the confirmed new power plants in the UK will take a similar approach with the safety case being a core element.

3.2.3. Demonstration of acceptable levels of risk

The UK safety–critical industries included in the review have all adopted the concept of "reasonable practicability" to demonstrate that hazards have been controlled effectively. This is based on the Health & Safety at Work, etc. Act 1974 (Health and Safety at Work etc, 1974) and the guidance developed by the HSE on "Reducing Risk: Protecting People" (Health and Safety Executive, 2001). The concept of reasonable practicability dates back to a legal case in 1949, in which the UK National Coal Board was defending a case in court following the death of an employee. In effect, this case established that operators of systems have a legal duty to reduce risk unless the sacrifices (in terms of money, effort, etc.) are grossly disproportionate to the expected benefits. This principle is known as *So far as is reasonably practicable* (SFAIRP) or *As Low As Reasonably Practicable* (ALARP) in its practical application. It requires from the operator a conscious and transparent decision about whether or not risk control measures are put in place. In current practice, the risk space is divided into three different regions: the region of unacceptable risk, where societal concerns are so great that the system cannot be operated; the region of negligible risk, where the risk is perceived to be so small that no further action is required to mitigate the risk; and the region of tolerable risk – this is the region where the risk is perceived to be tolerable, but only if further risk reduction is impracticable or if the associated costs are grossly disproportionate.

The HSE emphasises the importance of openness and transparency about how decisions are taken on the regulation of risk (Health and Safety Executive, 2001). A shared framework and clear guidance would enhance consistency and contribute to the spread of best practice. However, the evaluation of whether risk has been reduced as low as reasonably practicable can be complex in practice. The HSE recommends following industry-wide good practice, followed by the application of quantitative cost-benefit analyses (CBA) in cases where costs are claimed to be grossly disproportionate. However, the application of quantitative methods should be regarded only as supplementary information intended to inform decisions, but CBA cannot replace the qualitative assessment of risk and mitigation by experts (HSE).

While the concept of ALARP is widely accepted in the UK, its application has not been without problems and controversy. For example, the Nimrod review (Haddon-Cave, 2009) extensively dissects the ALARP judgements made concerning risks by the Nimrod Integrated Project Team, suppliers, and independent advisors, and questions whether the principle of ALARP was fully understood. In addition, both within the UK as well as in other countries there exists an argument questioning the ethics of ALARP. Such an opposing position calls for the implementation of safety measures capable of eliminating risk regardless of cost. If this is not the case then it is implied that a preventable accident is acceptable to organisations, the regulators and the government. For example, there had been much criticism of the decision not to adopt network wide Automatic Train Protection (ATP) systems in the UK railways, following a CBA undertaken by British Rail that suggested that the costs of ATP far outweighed its benefits. This ethical argument is

particularly powerful following accidents in which the victims had no immediate involvement, such as the population in the proximity of a site where toxic materials were released.

3.2.4. Practicality of review

The acceptance criteria for safety cases (i.e. the acceptable means of demonstrating safety rather than the acceptable level of safety) are poorly defined in many of the sectors reviewed in the study (e.g. automotive), and they also vary significantly between domains. The lack of clearly defined and understood acceptance criteria (e.g. to help assess whether a safety case is "compelling" as required by UK Ministry of Defence (2007) can challenge already stretched and understaffed regulatory authorities, which will also struggle to build assessment expertise due to differences between the acceptance criteria, safety arguments and items of evidence submitted for each safety case (Leveson, 2011). The lack of adequate funding of the regulatory authority is a key concern and threat to the successful adoption of the safety case approach. Steinzor even argues that the US petrochemical industry should not adopt the UK safety case regime because the American regulator was not adequately resourced (Steinzor, 2011).

The freedom offered within a goal-based safety case regime necessitates strong review (including regulatory review). Historically, there has been more emphasis on the development than the review of safety case arguments and evidence. For example, for safety case development, there is a well-documented body of work on safety argument patterns and templates that support the reuse of common styles of reasoning. Similarly, there are established approaches to the representation of safety arguments (e.g. Goal Structuring Notation GSN and Claims-Arguments-Evidence CAE). However, increasingly more approaches are being proposed for the review of safety cases. This is taking the form of qualitative review (Ayoub et al., 2012), formal mathematical analysis (Rushby, 2010) and quantitative analysis (Rae et al., 2014; Denney et al., 2011), including approaches that help reviewers in identifying argument fallacies (Greenwel, 2006), sources of uncertainty and counter evidence (Hawkins et al., 2011). Without clearly identified techniques and principles for safety case review (such as the Safety Assessment Principles defined in the UK Nuclear domain (Office for Nuclear Regulation, 2014a) there might be justified concerns about the confidence that can be placed in the safety case and safety case review.

3.2.5. Evidence of effectiveness

The review recorded that safety cases have not been adopted based on empirical evidence of effectiveness in industry. Instead, they have been adopted based upon the face validity that explicitly communicating the safety reasoning and evidence for a system is better than keeping this reasoning implicit. Apart from mostly academic case studies and industrial papers reporting anecdotal evidence, there is no empirical evidence that regulation based upon a safety case approach is more effective than regulation that does not require the explicit production of safety cases (Leveson, 2011; Wassyng et al., 2011; Hopkins, 2012). In fact, the airborne side of civil aviation, known for its rigorous and transparent safety practices and extremely low rates of accidents, does not require safety cases to be produced as part of its certification regime. The same can be said about certain defence systems in the US (Leveson, 2011). A review on the effectiveness of the COMAH regulations (that require safety cases) concluded that there was no direct evidence that the introduction of the regulations had resulted in a reduction in accident risks (HSE, 2006a). Serious criticisms were also raised by the Haddon-Cave review into the Nimrod accident concerning safety case practices, regarding both the construction and assessment of safety cases (Haddon-Cave, 2009).

On the other hand, a study that reviewed safety case practices in the oil and gas sector in New Zealand and Australia suggested that despite the shortcomings in implementation, the safety case approach was still accepted as the most effective way to managing safety in the sector (Fitzgerald et al., 2010). Further empirical evidence, in the form of controlled experiments, case studies or observational studies, is needed to validate specific claims of successful or cost-effective use of safety cases in industry, while noting the wider foundational issue concerning the need for appropriate evaluation approaches for empirically validating the use of safety analysis and assurance techniques in industry.

4. Safety case use in healthcare

Healthcare is a broad and complex industry including stakeholders and products as diverse as drugs and medicines, medical devices, health information technologies, and services provided by actors across organisational boundaries. It is often a fragmented and mixed economy made up of both private and public service providers. At present there is little experience with the safety case approach in healthcare (Sujan et al., 2015).

4.1. Role of the regulator

In the UK a number of different authorities are providing regulatory oversight, and they are following their own standards and regulatory principles. The only regulatory authority in the UK healthcare domain that requires the submission of safety cases is the Health and Social Care Information Centre (HSCIC). HSCIC requires manufacturers and operators of health informatics products in the NHS to develop and submit a Clinical Safety Case. The clinical safety case is based on the safety case principles described in the defence sector standard Def Stan 00-56.

4.2. Drivers: medical device and health information technology failures

In the UK, learning from other industries, in particular from the defence sector, has prompted interest in the safety case approach. This has given rise to guidance issued by NHS Connecting for Health (now part of HSCIC) on Clinical Safety Cases for health informatics products (Health and Care Information Centre, 2013a, 2013b). This was on the back of a report commissioned by the Deputy Chief Medical Officer, which looked at the approach to patient safety within the National Programme for IT (NPfIT). The report was prepared on behalf of and published by the National Patient Safety Agency in 2004 (National Patient Safety Agency, 2004). The report suggested that safety had not been identified as a driver for the programme and that there were neither formal risk assessment nor formal clinical safety management systems in place. The report concluded that NPfIT did not address safety in a structured and proactive way as other safety–critical industries would do. Learning from industrial safety standards, in particular IEC 61508 (IEC, 2010a) and Def-Stan-0056 (UK Ministry of Defence, 2007), and the engagement in standardisation activities, such as IEC 80001 on risk management for IT networks incorporating medical devices (IEC, 2010b), led to the implementation of a Clinical Safety Management System Approach, and the publication of two standards on risk management for the manufacture, deployment and use of health software aimed at both manufacturers and users (Health and Care Information Centre, 2013a, 2013b).

Another significant development has taken place in the USA, where the Food and Drug Administration (FDA) issued guidance for infusion pumps (FDA, 2014), which includes an assurance case approach that is built on the traditional safety case principle. With

this approach, the FDA aims to take a more proactive and comprehensive approach to preventing safety problems.

The FDA states that between 2005 and 2009 they had received over 56,000 reports of adverse events associated with the use of infusion pumps (FDA, 2014). These safety problems were the key driver behind the Infusion Pump Improvement initiative and the inclusion of the assurance case concept in the guidance. As the FDA does not have any experience with this concept, it has been limited to one type of medical device that is perceived to be particularly high risk.

4.3. Demonstration of acceptable levels of risk

In the NHS, and more generally in healthcare, the notion of acceptable levels of risk is not well established. Safety management is largely driven by analysis of outcome measures in a reactive fashion. Where risks are identified in a proactive fashion, improvement teams are left to their own devices as to which risks they should address, and the extent to which risks should be reduced. As a result, practice is extremely variable across the health system, and it is lacking in consistency and transparency. While healthcare providers need to maintain a risk register they do not normally need to demonstrate that risks have been reduced to acceptable levels.

There has been recent research on the development of safety cases for more general healthcare processes, such as handover from the day care team to the night care team in hospitals (Sujan et al., 2015). The aim of the research was to support healthcare organisations in thinking proactively about risks in their processes, and to facilitate their decision-making processes around potential risk reduction interventions. However, the research stopped short of specifying acceptable levels of risk, and the safety case was used as an improvement and communication tool rather than for regulatory purposes.

4.4. Practicality of review

There are few examples of safety cases in the healthcare domain publicly available. It is, therefore, difficult to determine how organisations and regulators are coping with the development and review of safety cases. The FDA requires submission of assurance cases only for one specific type of medical device, because they do not yet possess the required skills and experience to introduce the requirement for safety cases at scale. The HSCIC recruited a number of safety engineers with background from other industries to help set up the requirement for the submission of Clinical Safety Cases, and to provide education and training to manufacturers and healthcare providers.

4.5. Evidence of effectiveness

Since safety cases have not been used much in healthcare there is no evidence about their effectiveness available. The FDA has not published any updates about infusion pump incident rates following the introduction of the requirement for the submission of an assurance case. Similarly, no information is available from HSCIC about the effectiveness of Clinical Safety Cases in reducing the risk associated with the use of health informatics products.

5. Discussion

The review of safety case practices across UK industries suggests that safety cases are an accepted means of demonstrating that systems are meeting regulatory expectations and that they can be regarded as acceptably safe with reasonable confidence. The review identified five themes around the role of the regulator, the drivers behind the adoption of safety cases, the problem of determining acceptable levels of risk, the difficulties of regulatory review of complex technical safety case reports, and the lack of empirical evidence about the effectiveness of safety cases for improving safety performance. In healthcare, the interest in goal-based regulation and safety cases has been much more recent, and there is little established experience with the approach (Sujan et al., 2015).

Regulatory bodies play a key role by setting a mandate for industry on the one hand, and by providing guidance and advice on the other hand. However, the industry reviews also suggest that the introduction of goal-based regulation and the requirements for safety cases sometimes caused confusion due to lack of experience and expertise (HSE). In the National Health Service (NHS) in England there are a number of different regulatory bodies active, all with different and sometimes overlapping areas of oversight, and, crucially, different regulatory approaches. While, for example, some bodies require adherence to certain risk management standards, others rely largely on on-site inspection and retrospective quality and safety data pertaining to serious untoward events (NHS, 2015) and a set of common forms of patient harms (Power et al., 2012). Regulatory bodies might need to engage in a discussion and joint effort in order to transition from largely prescriptive and reactive regulatory approaches towards a more goal-based and proactive approach. For this to work in practice, there is a need for inspectors and guidance developers to have a thorough understanding of proactive risk management approaches. This might require targeted education that enables, for example, inspectors to ask the right questions, and assessors to look for adequate arguments and corresponding evidence. In addition, a suitable communication tool to facilitate the interaction between regulators and healthcare organisations around risk is required. Safety cases might be a potential candidate to facilitate this.

At the core of UK safety case practices is the ALARP principle that provides a shared framework for justification of safety. While arguably sometimes difficult to apply in practice (Haddon-Cave, 2009), this approach has none the less brought consistency and transparency to the different industries. In healthcare no comparable common notion of acceptable levels of risk and reasonable practicability exists. At present, healthcare organisations do not possess systematic processes or criteria that enable them to determine in a consistent and transparent way whether risks should be reduced further and how the trade-off between cost and risk reduction should be managed. As a result, the way risks are approached varies significantly and relies often on individual judgement (Sujan et al., 2015). The NHS and other healthcare systems face challenges that are different from the established safety–critical industries, and there is a duty to provide care to an aging population with increasingly complex health needs while at the same time reducing the burden on the taxpayer. It might be argued that a strict principle, such as ALARP, cannot be implemented within the financial climate of modern healthcare systems. However, it might be possible to start a dialogue and build a common framework around how healthcare providers and the healthcare system as a whole would like to treat patient safety risk in a consistent way. A main prerequisite for starting such a process is a better understanding of proactive, risk-based approaches among stakeholders in healthcare. Further education is required to provide a more proactive mindset that shifts from the consideration of outcomes only towards a risk-based perspective. There is an opportunity to use safety cases to facilitate this process by developing explicit accounts of the risks that are present in the system (Sujan et al., 2015). However, healthcare providers require assurance from the regulators that such an exposition of risk – rather than the demonstration of safety – would not have negative repercussions (Health Foundation, 2014).

Safety cases have face validity, but there is little published evidence of their direct contribution to safety performance in safety–critical industries (Leveson, 2011; Steinzor, 2011). While it could be argued that this may be impossible to produce given the complexity and dynamism of the industries, this opens up the approach to criticism and may make its adoption in healthcare more difficult. In healthcare, there is arguably a strong preference for "evidence-based" approaches. There is a risk that safety cases could be regarded as an intervention with associated costs and unclear evidence about their effectiveness. In addition to education about risk, there is, therefore, a need to produce and communicate more compelling empirical evidence about the contribution of safety cases to proactive safety management practices and to safety performance.

6. Conclusions

The failings at Mid Staffordshire and the media coverage around the extent of unnecessary patient harm and suffering shocked both healthcare professionals as well as the public. There is agreement that healthcare providers have to become more proactive, and that they should seek to adopt more rigorous patient safety management practices. Healthcare systems and policy makers are looking at other industries for lessons about effective safety management. Often the transfer of lessons from safety–critical industries to healthcare is difficult due to the different organisational, cultural and regulatory contexts.

Safety cases have the potential to support healthcare providers in setting up more proactive and structured safety management systems. However, the level of maturity of safety management practices in healthcare is arguably lower than in other safety–critical industries, and healthcare systems do not usually operate with similar shared frameworks for communicating and justifying safety based on common notions of acceptable levels of risk and reasonable practicability. Adopting safety cases in healthcare within a goal-based regulatory framework to demonstrate that systems are acceptably safe, as is practice in UK safety–critical industries, might prove to be an uphill struggle. It might not even be the most reasonable approach, at least in the short-term. A more promising route might be to identify possible ways in which safety cases might contribute to a proactive mindset and discussion about risk in healthcare. Safety cases might support healthcare organisations in developing an understanding and an exposition of their current levels of risk, and such an exposition of risk might be a useful communication tool between healthcare providers and regulators. This requires a certain level of trust between healthcare providers and regulators, and a commitment to work together towards reducing the risk to patients.

Many of these concepts around risk and safety cases are still alien to stakeholders in healthcare. Healthcare providers and regulators require access to education and guidance that takes into account the specifics of healthcare as an industry. In addition, further research is required to provide evidence about the effectiveness of safety cases and the costs involved with the approach. Such evidence would enable stakeholders in healthcare to make a more informed decision about regulatory approaches and organisational safety management.

Based on the above discussion we identify the following recommendations:

For healthcare regulatory bodies – Regulatory bodies should work together in an effort to harmonise their regulatory approaches and to transition towards a proactive, goal-based regulatory framework.

For healthcare providers – Healthcare organisations should develop proactively an explicit account of their patient safety risks, and consider documenting these in a safety case.

For healthcare systems – National healthcare systems should develop healthcare-specific notions of acceptable levels of risk in order to provide a consistent and transparent framework for managing patient safety risk.

For safety science professionals and researchers – Safety professionals should develop healthcare-specific training and guidance on proactive risk management and the role of safety cases for healthcare providers and regulatory bodies. Safety science researchers should design research studies that can provide empirical evidence of the contribution of safety cases to proactive safety management practices and safety performance.

Acknowledgements

This work was funded by a research grant from the Health Foundation (Registered Charity Number: 286967). Robin Bloomfield, Nick Chozos, David Embrey, Jamie Henderson, Floor Koornneef and Alberto Pasquini were part of the research team. George Cleland and John Medhurst provided input to reviews on regulatory practices in healthcare and railways. We would like to thank the participants of the stakeholder workshop. We also acknowledge the discussions with members of the Medical Devices Group of EWICS TC7.

References

Apkon, M., Leonard, J., Probst, L., DeLizio, L., Vitale, R., 2004. Design of a safer approach to intravenous drug infusions: failure mode effects analysis. Qual. Safety Health Care 13, 265–271.

Ayoub, A., Kim, B., Lee, I., Sokolsky, O., 2012. A systematic approach to justifying sufficient confidence in software safety arguments. In: Ortmeier, F., Daniel, P. (Eds.), Computer Safety, Reliability, and Security. Springer, Berlin, Heidelberg, pp. 305–316.

Baker, G.R., Norton, P.G., Flintoft, V., Blais, R., Brown, A., Cox, J., et al., 2004. The Canadian Adverse Events Study: the incidence of adverse events among hospital patients in Canada. Can. Med. Assoc. J. 170, 1678–1686.

Barker, S., Kendall, I., Darlison, A., 1997. Safety cases for software-intensive systems: an industrial experience report. In: Daniel, P. (Ed.), Safe Comp 97. Springer, London, pp. 332–342.

Birch, J., Rivett, R., Habli, I., Bradshaw, B., Botham, J., Higham, D., et al., 2013. Safety cases and their role in ISO 26262 functional safety assessment. In: Bitsch, F., Guiochet, J., Kaâniche, M. (Eds.), Computer Safety, Reliability, and Security. Springer, Berlin, Heidelberg, pp. 154–165.

Bishop, P., Bloomfield, R., Guerra, S., 2004. The future of goal-based assurance cases. Proc. Workshop Assurance Cases, 390–395.

Bloomfield, R., Chozos, N., Embrey, D., Henderson, J., Kelly, T., Koornneef, F., et al., 2012a. Using Safety Cases in Industry and Healthcare. Health Foundation, London.

Bloomfield, R., Chozos, N., Embrey, D., Henderson, J., Kelly, T., Koornneef, F., et al., 2012b. Supplements to Using Safety Cases in Industry and Healthcare. Health Foundation, London.

Brennan, T.A., Leape, L.L., Laird, N.M., Hebert, L., Localio, A.R., Lawthers, A.G., et al., 1991. Incidence of adverse events and negligence in hospitalized patients. New England J. Med. 324, 370–376.

Burgmeier, J., 2002. Failure mode and effect analysis: an application in reducing risk in blood transfusion. Joint Comm. J. Qual. Improv. 28, 331–339.

Carruthers, I., Phillip, P., 2006. Safety First: A Report for Patients, Clinicians and Healthcare Managers. National Patient Safety Agency, London.

Chen, Y., Lawford, M., Wang, H., Wassyng, A., 2014. Insulin pump software certification. In: Gibbons, J., MacCaull, W. (Eds.), Foundations of Health Information Engineering and Systems. Springer, Berlin, Heidelberg, pp. 87–106.

Chinneck, P., Pumfrey, D., Kelly, T., 2004. Turning up the HEAT on safety case construction. In: Redmill, F., Anderson, T. (Eds.), Practical Elements of Safety. Springer, London, pp. 223–240.

Davis, P., Lay-Yee, R., Briant, R., Ali, W., Scott, A., Schug, S., 2002. Adverse events in New Zealand public hospitals I: occurrence and impact. New Zealand Med. J. 115, U271.

de Vries, E.N., Ramrattan, M.A., Smorenburg, S.M., Gouma, D.J., Boermeester, M.A., 2008. The incidence and nature of in-hospital adverse events: a systematic review. Qual. Safety Health Care 17, 216–223.

Denney, E., Pai, G., Habli, I., 2011. Towards measurement of confidence in safety cases. In: Proceedings of the 2011 International Symposium on Empirical Software Engineering and Measurement. IEEE Computer Society, pp. 380–383.

Department of Health, 2006. An Organisation with a Memory. The Stationery Office, London.

Dependability Research Group University of Virginia. Safety Cases: Repository.
Despotou, G., White, S., Kelly, T.P., Ryan, M., 2012. Introducing safety cases for health IT. In: Proceedings of the 4th International Workshop on Software Engineering in Health Care. ACM, Zurich.
Eurocontrol, 2006. Safety Case Development Manual.
Evans, A., 2007. Rail safety and rail privatisation in Britain. Accid. Anal. Prevent. 39, 510–523.
FDA, 2014. Infusion Pumps Total Product Life Cycle: Guidance for Industry and FDA staff. Rockville, MD.
Fennell, D., 1998. Investigation into the King's Cross Underground Fire. The Stationery Office, London.
Fitzgerald, B., Breen, P.M., Patrick, J.H., 2010. Has the Safety Case Failed? In: SPE Asia Pacific Oil and Gas Conference. Society of Petroleum Engineers, Brisbane.
Francis, R., 2013. Report of the Mid Staffordshire NHS Foundation Trust Public Inquiry.
Greenwell, W., 2006. A taxonomy of fallacies in system safety arguments. In: Proceedings of the 2006 International System Safety Conference.
Habli, I., Kelly, T., 2006. Process and product certification arguments: getting the balance right. SIGBED Rev. 3, 1–8.
Habli, I., Ibarra, I., Rivett, R., Kelly, T., 2010. Model-Based Assurance for Justifying Automotive Functional Safety. SAE 2010 World Congress. Detroit.
Haddon-Cave, C., 2009. The Nimrod Review: An Independent Review into the Broader Issues Surrounding the Loss of the RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006. The Stationery Office, London.
Hawkins, R., Kelly, T., Knight, J., Graydon, P., 2011. A new approach to creating clear safety arguments. In: Dale, C., Anderson, T. (Eds.), Advances in Systems Safety. Springer, London, pp. 3–23.
Hawkins, R., Habli, I., Kelly, T., McDermid, J., 2013. Assurance cases and prescriptive software safety certification: a comparative study. Safety Sci. 59, 55–71.
Health Foundation, 2014. Exploring the Potential Use of Safety Cases in Health Care. Health Foundation, London.
Health & Social Care Information Centre, 2013a. Clinical Risk Management: Its Application in the Manufacture of Health IT Systems – Implementation Guidance.
Health & Social Care Information Centre, 2013b. Clinical Risk Management: Its Application in the Deployment and Use of Health IT Systems – Implementation Guidance.
Health and Safety at Work etc. Act, 1974.
Health and Safety Executive, 2001. Reducing Risk: Protecting People.
Hidden, A., 1989. Investigation of the Clapham Junction Railway Accident. The Stationery Office, London.
Hopkins, A., 2012. WP 87 – Explaining "Safety Case". National Research Centre for OHS Regulation, Canberra.
HSE, 1999. Control of Major Accident Hazards Regulations 1999 (COMAH).
HSE, 2006a. Impact Evaluation of the Control of Major Accident Hazards (COMAH) Regulations 1999. HSE Books, London.
HSE, 2006b. Developing Process Safety Indicators. HSE Books, London.
HSE. ALARP "at a glance".
HSE. COMAH – Safety Report Assessment Manual (V2).
IEC, 2010a. 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Geneva.
IEC, 2010b. IEC 80001-1:2010 Application of Risk Management for IT-networks Incorporating Medical Devices – Part 1: Roles, Responsibilities and Activities. IEC, Geneva.
Kohn, L.T., Corrigan, J.M., Donaldson, M.S., 2000. To Err Is Human: Building a Safer Health System. The National Academies Press, Washington.
Layfield, Sir F., 1987. Sizewell B Public Inquiry Report. London.
Leveson, N., 2011. The use of safety cases in certification and regulation. J. Syst. Safety, 47.
Maguire, R., 2006. Safety Cases and Safety Reports. Ashgate, Aldershot.
MISRA, 2007. Guidelines for Safety Analysis of Vehicle based Programmable Systems. Nuneaton.
National Patient Safety Agency, 2004. Review of NPfIT with Regard to Patient Safety. Department of Health, London.
NHS England Patient Safety Domain, 2015. Revised Never Events Policy and Framework. NHS England, London.
Office for Nuclear Regulation, 2013. The Purpose, Scope and Content of Safety Cases.
Office for Nuclear Regulation, 2014a. Safety Assessment Principles (SAPs).
Office for Nuclear Regulation, 2014b. Technical Assessment Guides (TAGs).
Ovretveit, J., 2009. Does Improving Quality Save Money? Health Foundation, London.
Power, M., Stewart, K., Brotherton, A., 2012. What is the NHS safety thermometer? Clin. Risk 18, 163–169.
Rae, A., Alexander, R., McDermid, J., 2014. Fixing the cracks in the crystal ball: a maturity model for quantitative risk assessment. Reliab. Eng. Syst. Safety 125, 67–81.
Ray, A., Cleaveland, R., 2013. Constructing safety assurance cases for medical devices. Assurance Cases for Software-Intensive Systems (ASSURE). In: 2013 1st International Workshop on 2013, pp. 40–45.
Rushby, J., 2010. Formalism in safety cases. In: Dale, C., Anderson, T. (Eds.), Making Systems Safer. Springer, London, pp. 3–17.
Steinberger, D.M., Douglas, S.V., Kirschbaum, M.S., 2009. Use of failure mode and effects analysis for proactive identification of communication and handoff failures from organ procurement to transplantation. Progr. Transpl. (Aliso Viejo, Calif) 19, 208–214, quiz 15.
Steinzor, R., 2011. Lessons from the North Sea: Should "Safety Cases" come to America? Boston Coll. Environ. Affairs Law Rev. 38, 417–444.
Sujan, M.A., Felici, M., 2012. Combining failure mode and functional resonance analyses in healthcare settings. Comput. Safety, Reliab., Secur., 364–375
Sujan, M.A., Koornneef, F., Voges, U., 2007. Goal-based safety cases for medical devices: opportunities and challenges. Comput. Safety, Reliab., Secur., 14–27
Sujan, M.A., Koornneef, F., Chozos, N., Pozzi, S., Kelly, T., 2013. Safety cases for medical devices and health IT: involving healthcare organisations in the assurance of safety. Health Informatics J. 19, 165–182.
Sujan, M., Spurgeon, P., Cooke, M., Weale, A., Debenham, P., Cross, S., 2015. The development of safety cases for healthcare services: practical experiences, opportunities and challenges. Reliab. Eng. Syst. Safety 140, 200–207.
The Honourable Lord Cullen, 1990. Public Inquiry into the Piper Alpha Disaster. London.
The Offshore Installations (Safety Case) Regulations, 2005.
The Railways (Safety Case) Regulations, 1994.
Thomas, E.J., Studdert, D.M., Burstin, H.R., Orav, E.J., Zeena, T., Williams, E.J., et al., 2000. Incidence and types of adverse events and negligent care in Utah and Colorado. Med. Care 38, 261–271.
UK Ministry of Defence, 1996. Joint Service Publication JSP 430: MoD Ship Safety Management. The Stationery Office, London.
UK Ministry of Defence, 2002. Joint Service Publication JSP 454: Procedures for Land Systems Equipment Safety Assurance. The Stationery Office, London.
UK Ministry of Defence, 2003. Joint Service Publication JSP 553: Military Airworthiness Regulations. The Stationery Office, London.
UK Ministry of Defence, 2007. Defence Standard 00-56: Safety Management Requirements for Defence Systems. The Stationery Office, London.
Vincent, C., Neale, G., Woloshynowych, M., 2001. Adverse events in British hospitals: preliminary retrospective record review. BMJ (Clinical research ed) 322, 517–519.
Wassyng, A., Maibaum, T., Lawford, M., Bherer, H., 2011. Software certification: is there a case against safety cases? In: Calinescu, R., Jackson, E. (Eds.), Foundations of Computer Software Modeling, Development, and Verification of Adaptive Systems. Springer, Berlin, Heidelberg, pp. 206–227.
Workshop on Safety Cases – Lessons from Industry and Application in Healthcare, 2011. <http://www2.warwick.ac.uk/fac/med/staff/sujan/research/safety_case_review/wp3_workshop/>